AMENDED IN ASSEMBLY APRIL 24, 2014

AMENDED IN ASSEMBLY MARCH 28, 2014

california legislature—2013–14 regular session

ASSEMBLY BILL No. 1710

Introduced by Assembly Members Dickinson and Wieckowski

February 13, 2014

An act to amend Sections 1798.81.5, 1798.82, 1798.84, and 1798.85 of, and to add Sections 1724.4 and 1724.6 to, the Civil Code, relating to personal information privacy.

legislative counsel's digest

AB 1710, as amended, Dickinson. Personal information: privacy.

Existing law requires a person or business conducting business in California that owns or licenses computerized data that includes personal information, as defined, to disclose, as specified, a breach of the security of the system or data following discovery or notification of the security breach to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This bill would instead require a person or business conducting business in California that owns or licenses computerized ~~or noncomputerized~~ data that contains personal information to disclose, as specified, a breach of the security of the system or data following discovery or notification of the security breach to any California resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person *unless the data was encrypted, as specified*. If the person or business was the source of the breach, the bill would require the person or business to offer to provide appropriate identity theft prevention and mitigation services, *if any,* to the affected person at no cost for not less than 24 months if the breach exposed or may have exposed specified personal information. The bill would also require a person or business that maintains but does not own the data to notify the persons affected ~~within 15 days of the breach using specified methods~~ *at the same time that notice is given to the owner or licensee, as specified.*

This bill would prohibit a person or business that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device, from storing, retaining, sending, or failing to limit access to payment-related data, as defined, retaining a primary account number, or storing sensitive authentication data subsequent to an authorization, as specified, unless a specified exception applies. The bill would make a person or business liable for the reimbursement of all reasonable and actual costs of providing notice of a breach of the security of a system or data following discovery or notification of the security breach to any California resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person *unless the data was encrypted, as specified,* and for the reasonable and actual cost of card replacement as a result of a breach, to the owner or licensee of the information. The bill would authorize this liability to be excused, in whole or in part, if the person or business, can demonstrate compliance with specified provisions at the time of the breach.

Existing law requires a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

This bill would expand these provisions to businesses that own, license, or maintain personal information about a California resident, as specified.

~~Existing law authorizes any customer injured by a violation of specified provisions relating to customer records to institute a civil action to recover damages and penalties, as specified.~~

~~This bill would, in addition to any other available remedies, authorize a public prosecutor to bring an action to recover a civil penalty not exceeding $500, or for a willful, intentional, or reckless violation not exceeding $3,000, per violation.~~

Existing law prohibits a person or entity, with specified exceptions, from publicly posting or displaying an individual's social security number or doing certain other acts that might compromise the security of an individual's social security number, unless otherwise required by federal or state law.

This bill would also, *except as specified,* prohibit the sale, advertisement for sale, or offer to sell of an individual's social security number. The bill would, in addition to any other available remedies for a violation of these provisions, authorize a public prosecutor to bring an action to recover a civil penalty not exceeding $500 per violation.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1724.4 is added to the Civil Code, to read:

1724.4. (a) In addition to being subject to the provisions of Title 1.81 (commencing with Section 1798.80) of Part 4, a person or business that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device shall not do any of the following:

(1) Store payment-related data, unless the person or business complies with both of the following:

(A) The person or business has a payment data retention and disposal policy that limits the amount of payment-related data and the time that data is retained to only the amount and time required for business, legal, or regulatory purposes as explicitly documented in the policy.

(B) The person or business retains payment-related data only for a time period and in a manner explicitly permitted by the policy.

(2) Store sensitive authentication data subsequent to an authorization, even if that data is encrypted. Sensitive authentication data includes all of the following:

(A) The full contents of any data track from a payment card or other payment device.

(B) The card verification code or any value used to verify transactions when the payment device is not present.

(C) The personal identification number (PIN) or the encrypted PIN block.

(3) Store any payment-related data that is not needed for business, legal, or regulatory purposes.

(4) Store any of the following data elements:

(A) Payment verification code.

(B) Payment verification value.

(C) PIN verification value.

~~(D) Social security number.~~

~~(E) Driver's license number.~~

(5) Retain the primary account number unless retained in a manner consistent with the other requirements of this subdivision and in a form that is unreadable and unusable by unauthorized persons anywhere it is stored.

(6) Send payment-related data over open, public networks unless the data is encrypted using strong cryptography and security protocols or otherwise rendered indecipherable.

(7) Fail to limit access to payment-related data to only those individuals whose job requires that access.

(b) (1) This section shall not apply to any person or business subject to Sections 6801 to 6809, inclusive, of Title 15 of the United States Code and state or federal statutes or regulations implementing those sections, if the person or business is subject to compliance oversight by a state or federal regulatory agency with respect to those sections.

(2) Nothing in this section shall prohibit a person or business that sells goods or services to any California resident and accepts as payment a credit card, debit card, or other payment device from storing payment-related data for the sole purpose of processing ongoing or recurring payments, provided that the payment-related data is maintained in accordance with this section.

(c) For purposes of this section, "payment-related data" means any computerized information described in subdivision (h) of Section 1798.82, whether individually or in combination with any other information described in that paragraph.

SEC. 2. Section 1724.6 is added to the Civil Code, to read:

1724.6. (a) A person or business subject to Section 1724.4 shall be liable for the reimbursement of all reasonable and actual costs of providing notice pursuant to subdivision (a) of Section 1798.82 and for the reasonable and actual cost of card replacement as a result of a breach described in that section, to the owner or licensee of the information.

(b) The liability of a person or business subject to Section 1724.4 to reimburse the owner or licensee may be excused, in whole or in part, if the person or business can demonstrate compliance with all provisions of Section 1724.4 at the time of the breach of security of the system.

SEC. 3. Section 1798.81.5 of the Civil Code is amended to read:

1798.81.5. (a) (1) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.

(2) For the purpose of this section, the terms "own" and "license" include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term "maintain" includes personal information that a business maintains but does not own or license.

(b) A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(d) For purposes of this section, the following terms have the following meanings:

(1) "Personal information" means an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(2) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.

(3) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(e) The provisions of this section do not apply to any of the following:

(1) A provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1).

(2) A financial institution as defined in Section 4052 of the Financial Code and subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code.

(3) A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

(4) An entity that obtains information under an agreement pursuant to Article 3 (commencing with Section 1800) of Chapter 1 of Division 2 of the Vehicle Code and is subject to the confidentiality requirements of the Vehicle Code.

(5) A business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section. Compliance with that state or federal law shall be deemed compliance with this section with regard to those subjects. This paragraph does not relieve a business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

SEC. 4. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) A person or business that conducts business in California, and that owns or licenses computerized~~ or noncomputerized~~ data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person *unless the data was encrypted in conformance with the Advanced Encryption Standard of the National Institute of Standards and Technology, Federal Information Processing Standards Publication 197, as amended from time to time*. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) (1) A person or business that maintains computerized~~ or noncomputerized~~ data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(2) In addition to notifying the owner *or licensee* of the data, the person or business that maintains the data shall notify persons affected by the breach~~ within 15 days of the breach using the following methods:~~ *at the same time that notice is given to the owner or licensee by*

~~(A) Email~~ *United States mail if the person or business has a mailing address for the subject persons or email* notice if the person or business has an email address for the subject persons. *If the subject persons cannot be notified by mail or email, the person or business shall provide notice by the following methods:*

~~(B)~~

(A) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains an Internet Web site page, for at least 30 days.

~~(C)~~

(B) Notification to major statewide media.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services~~, such as credit monitoring,~~ *if any,* shall be provided at no cost to the affected person for not less than 24 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in *subparagraphs (A) and (B) of* paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (j) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized ~~or noncomputerized~~ data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, *when either the name or the data elements are not encrypted in conformance with the Advanced Encryption Standard of the National Institute of Standards and Technology, Federal Information Processing Standards Publication 197, as amended from time to time*:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, “health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

(j) For purposes of this section, “notice” may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 5. Section 1798.84 of the Civil Code is amended to read:

1798.84. (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.

~~(b) In addition to any other available remedies for a violation of this title, a public prosecutor authorized pursuant to Section~~

~~17204 of the Business and Professions Code may bring an action to recover a civil penalty not exceeding five hundred dollars ($500) per violation, or, in the case of a willful, intentional, or reckless violation, a penalty not exceeding three thousand dollars ($3,000) per violation.~~

~~(c)~~

(b) Any customer injured by a violation of this title may institute a civil action to recover damages.

~~(d)~~

(c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.

~~(e)~~

(d) Unless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively.

~~(f)~~

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

~~(g)~~

(f) (1) A cause of action shall not lie against a business for disposing of abandoned records containing personal information by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

(2) The Legislature finds and declares that when records containing personal information are abandoned by a business, they

often end up in the possession of a storage company or commercial landlord. It is the intent of the Legislature in paragraph (1) to create a safe harbor for such a record custodian who properly disposes of the records in accordance with paragraph (1).

~~(h)~~

(g) A prevailing plaintiff in any action commenced under Section 1798.83 shall also be entitled to recover his or her reasonable attorney's fees and costs.

~~(i)~~

(h) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

SEC. 6. Section 1798.85 of the Civil Code is amended to read:

1798.85. (a) Except as provided in this section, a person or entity may not do any of the following:

(1) Publicly post or publicly display in any manner an individual's social security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public.

(2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity.

(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.

(4) Require an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.

(5) Print an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. Notwithstanding this paragraph, social security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security number. A social security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other

mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

(6) Sell, advertise for sale, or offer to sell an individual's social security number *except where the social security number is incidental to the transaction*.

(b) This section does not prevent the collection, use, or release of a social security number as required by state or federal law or the use of a social security number for internal verification or administrative purposes.

(c) This section does not prevent an adult state correctional facility, an adult city jail, or an adult county jail from releasing an inmate's social security number, with the inmate's consent and upon request by the county veterans service officer or the United States Department of Veterans Affairs, for the purposes of determining the inmate's status as a military veteran and his or her eligibility for federal, state, or local veterans' benefits or services.

(d) This section does not apply to documents that are recorded or required to be open to the public pursuant to Chapter 3.5 (commencing with Section 6250), Chapter 14 (commencing with Section 7150) or Chapter 14.5 (commencing with Section 7220) of Division 7 of Title 1 of, Article 9 (commencing with Section 11120) of Chapter 1 of Part 1 of Division 3 of Title 2 of, or Chapter 9 (commencing with Section 54950) of Part 1 of Division 2 of Title 5 of, the Government Code. This section does not apply to records that are required by statute, case law, or California Rule of Court, to be made available to the public by entities provided for in Article VI of the California Constitution.

(e) (1) In the case of a health care service plan, a provider of health care, an insurer or a pharmacy benefits manager, a contractor as defined in Section 56.05, or the provision by any person or entity of administrative or other services relative to health care or insurance products or services, including third-party administration or administrative services only, this section shall become operative in the following manner:

(A) On or before January 1, 2003, the entities listed in paragraph (1) shall comply with paragraphs (1), (3), (4), and (5) of subdivision (a) as these requirements pertain to individual policyholders or individual contractholders.

(B) On or before January 1, 2004, the entities listed in paragraph (1) shall comply with paragraphs (1) to (5), inclusive, of subdivision (a) as these requirements pertain to new individual policyholders or new individual contractholders and new groups, including new groups administered or issued on or after January 1, 2004.

(C) On or before July 1, 2004, the entities listed in paragraph (1) shall comply with paragraphs (1) to (5), inclusive, of subdivision (a) for all individual policyholders and individual contractholders, for all groups, and for all enrollees of the Healthy Families and Medi-Cal programs, except that for individual policyholders, individual contractholders and groups in existence prior to January 1, 2004, the entities listed in paragraph (1) shall comply upon the renewal date of the policy, contract, or group on or after July 1, 2004, but no later than July 1, 2005.

(2) A health care service plan, a provider of health care, an insurer or a pharmacy benefits manager, a contractor, or another person or entity as described in paragraph (1) shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of this article are implemented on or before the dates specified in this section.

(3) Notwithstanding paragraph (2), the Director of the Department of Managed Health Care, pursuant to the authority granted under Section 1346 of the Health and Safety Code, or the Insurance Commissioner, pursuant to the authority granted under Section 12921 of the Insurance Code, and upon a determination of good cause, may grant extensions not to exceed six months for compliance by health care service plans and insurers with the requirements of this section when requested by the health care service plan or insurer. Any extension granted shall apply to the health care service plan or insurer's affected providers, pharmacy benefits manager, and contractors.

(f) If a federal law takes effect requiring the United States Department of Health and Human Services to establish a national unique patient health identifier program, a provider of health care, a health care service plan, a licensed health care professional, or a contractor, as those terms are defined in Section 56.05, that complies with the federal law shall be deemed in compliance with this section.

(g) A person or entity may not encode or embed a social security number in or on a card or document, including, but not limited to, using a barcode, chip, magnetic strip, or other technology, in place of removing the social security number, as required by this section.

(h) This section shall become operative, with respect to the University of California, in the following manner:

(1) On or before January 1, 2004, the University of California shall comply with paragraphs (1), (2), and (3) of subdivision (a).

(2) On or before January 1, 2005, the University of California shall comply with paragraphs (4) and (5) of subdivision (a).

(i) This section shall become operative with respect to the Franchise Tax Board on January 1, 2007.

(j) This section shall become operative with respect to the California community college districts on January 1, 2007.

(k) This section shall become operative with respect to the California State University system on July 1, 2005.

(*l*) This section shall become operative, with respect to the California Student Aid Commission and its auxiliary organization, in the following manner:

(1) On or before January 1, 2004, the commission and its auxiliary organization shall comply with paragraphs (1), (2), and (3) of subdivision (a).

(2) On or before January 1, 2005, the commission and its auxiliary organization shall comply with paragraphs (4) and (5) of subdivision (a).

(m) In addition to any other available remedies for a violation of this title, a public prosecutor authorized pursuant to Section 17204 of the Business and Professions Code may bring an action to recover a civil penalty not exceeding five hundred dollars ($500) per violation.

O